UNITED STATES PATENT AND TRADEMARK OFFICE

mn

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,135	07/30/2003	Siani Lynne Pearson	B-5196 621146-3	1838

7590 03/12/2007
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/632,135	**Applicant(s)** PEARSON ET AL.	
	Examiner Samson B. Lemma	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 November 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12, 14-33 and 35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12, 14-33 and 35* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on November 22, 2006.

- Independent claims **14-15 and 35**; and dependent claims 16 and 22 are amended.
- Claims **13 and 34** are canceled
- No new claims are added.
- There are 6 independent claims namely, claims **1, 14-15,17, 23 and 35.**

Thus claims **1-12, 14-33 and 35** remains in the application/examined.

Response to Arguments

2. Applicant's remark/arguments filed on November 22, 2006 regarding **claims 1-12, 14-33 and 35** have been fully considered; and found to be persuasive but moot in view of new grounds of rejections.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. **Independent claims 1, 14-15,17, 23 and 35** are rejected under 35 U.S.C. 101 because the subject matter is directed to non-statutory subject matter.

5. **Claims 1, 14-15,17, 23 and 35** are directed to a method/apparatus and a system claims for validating the performance of a participant in an interactive computing environment. The examiner asserts that the limitation of the claims does not fall within the statutory classes listed in 35 USC 101; since the last limitation recited in

all the respective independent claims, "**and if it is then issuing a second challenge to test the integrity of an application run on the participant's computing device, and then making a decision concerning the participant's involvement in the computing environment**" wouldn't produce a tangible result.

Even though the last limitation of the respective independent claims are directed to a technological art, environment or machine which would result in a practical application producing **a concrete and useful result,** it does not produce **a tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.**

For instance, if the last limitation in the claim is only generating encryption/decryption key or comparing two results, with out transmitting, displaying or storing or performing some concrete result, by which the result is precisely identified or realized and perceived, the claim language is not generally considered to be producing tangible result.

By the same token, the last limitation recited as "making a decision concerning the participant's involvement in the computing environment" is not considered as producing a tangible result unless and otherwise the final limitation of the claim is some how either transmitting, storing or displaying, some concrete result. In other words the final limitation in the claim language has to be something, which is capable of being precisely identified or realized and perceived.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1-12, 14-33 and 35** are rejected under 35 U.S.C. 103(a) as being unpatentable over the publication with the title "Building A Foundation of Trust in the PC" (The Trusted Computing Platform Alliance) (hereinafter refereed as **Trusted Computing**) (Printed publication date: January, 2000) (Submitted with IDS) in view of **Jonathan Trostle (**hereinafter refereed as **Trostle**) (U.S. Patent No. 5,919,257)

8. **As per independent claims 1, 14-15, 17, 23 and 35 Trusted Computing discloses a method of validating the performance of a participant in an interactive computing environment,** *[See page 5, under the title "Remote Attestation up to page 6, first paragraph]* **comprising**:

Issuing a first challenge to a participant's computing device to determine whether the participant's computing device is trustworthy, *[See page 5, under the title "Remote Attestation, up to page 6, first paragraph] ("TCPA remote attestation allows an application **(the "challenger")** to trust a remote platform. This trust is built by obtaining integrity metrics for the remote platform, securely storing these metrics and then ensuring that the reporting of the metrics is secure. For example, before making content available to a subscriber, it is likely that a service provider will need to know that the remote platform **is trustworthy.** The service provider's platform (the "challenger") queries " the remote platform, meets the limitation "**issuing a first challenge to a participant's computing device to determine whether the participant's computing device is trustworthy,**" During system boot, the challenged platform creates a cryptographic hash of the system BIOS, using an algorithm to create a statistically unique identifier for the platform. The integrity metrics are then stored. When it receives the query from the challenger, the remote platform responds by digitally signing and then sending the integrity metrics. The digital* *signature prevents tampering and allows the challenger to verify the signature. If the signature is verified, the challenger can then determine whether the identity metrics are trustworthy meets the limitation of* ***"determining whether or not the participant's computing device is trustworthy"*** *If so, the challenger, in this case the service provider, can then deliver the content. It is important to note that the TCPA process does not make judgments regarding the integrity metrics. It merely reports the metrics and lets the challenger* ***make the final decision regarding the trustworthiness*** *of the remote platform.)*

Trusted Computing does not explicitly teach,

- Issuing a second challenge to test the integrity of an application run on the participant's computing device, and then making a decision concerning the participant's involvement in the computing environment.
- **However, in the same field of endeavor, Trostle on column** 7, lines 52-column 8, line 4, **discloses a method** of detecting **illicit changes to an executable program** in a networked computer workstation prior to execution of an operating system by the workstation, the method comprising the steps of: receiving a trusted hash value that is expected to be generated by hashing selected executable programs resident in the workstation if the selected executable programs have not been unauthorizedly changed; receiving a list of the selected executable programs resident in the workstation; hashing the selected executable programs resident in the workstation to calculate a computed hash value meets the limitation recited as **"Issuing a second challenge to test the integrity of an application run on the participant's computing device";** and comparing said computed hash value to said trusted hash value in order to detect illicit changes to the selected executable programs meets the limitation recited as "**and then making a decision concerning the**

participant's involvement in the computing environment."; [7, lines 52-column 8, line 4]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of issuing a second challenge to test the integrity of an application run on the participant's computing device, and then making a decision concerning the participant's involvement in the computing environment as per teachings of **Trostle** into the method as taught **Trusted Computing** for the purpose of creating more secure, comprehensive, user friendly intrusion detection system. [See "Trostle" the title and column 1, lines 38-61]

9. **As per claims 2-4, 18-20 and 24-26,the combination of Trusted Computing Trostle discloses a method as applied to claims above. Furthermore Trostle discloses a method, in which the second challenge tests for modification of the application. [7, lines 52-column 8, line 4]** *(Trostle on column 7, lines 52-column 8, line 4, discloses a method of detecting illicit changes to an executable program in a networked computer workstation prior to execution of an operating system by the workstation, the method comprising the steps of: receiving a trusted hash value that is expected to be generated by hashing selected executable programs resident in the workstation if the selected executable* ***programs have not been unauthorizedly changed****; receiving a list of the selected executable programs resident in the workstation; hashing the selected executable programs resident in the workstation to calculate a computed hash value meets the limitation "Issuing a second challenge to test the integrity of an application run on the participant's computing device"; and comparing said computed hash value to said trusted hash value in order to detect illicit changes to the selected executable programs meets the limitation "and then making a decision concerning the participant's involvement*

in the computing environment. And all together this meets the limitation recited as "second challenge tests for modification of the application.")

10. As per claims 5-8, 21-22 and 27-28 the combination of Trusted Computing Trostle discloses a method as applied to claims above. Furthermore Trostle discloses a method, in which in the first challenge the trustworthiness of the BIOS is validated, *[See page 5, under the title "Remote Attestation, up to page 6, first paragraph] ("TCPA remote attestation allows an application* ***(the "challenger")*** *to trust a remote platform. This trust is built by obtaining integrity metrics for the remote platform, securely storing these metrics and then ensuring that the reporting of the metrics is secure. For example, before making content available to a subscriber, it is likely that a service provider will need to know that the remote platform* ***is trustworthy.*** *The service provider's platform (the "challenger") queries " the remote platform, meets the limitation* ***"issuing a first challenge to a participant's computing device to determine whether the participant's computing device is trustworthy,"*** *During system boot, the challenged platform creates a cryptographic hash of the system BIOS, using an algorithm to create a statistically unique identifier for the platform. The integrity metrics are then stored. When it receives the query from the challenger, the remote platform responds by digitally signing and then sending the integrity metrics. The digital signature prevents tampering and allows the challenger to verify the signature. If the signature is verified, the challenger can then determine whether the identity metrics are trustworthy meets the limitation of* ***"determining whether or not the participant's computing device is trustworthy"*** *If so, the challenger, in this case the service provider, can then deliver the content. It is important to note that the TCPA process does not make judgments regarding the integrity metrics. It merely reports the metrics and lets the challenger* ***make the final decision regarding the trustworthiness*** *of the remote platform.)*

11. <u>As per claims 9-12,16, 29-33</u> the combination of Trusted Computing and Trostle discloses a method as applied to claims above. Furthermore Trostle discloses a method, in which the challenge is issued by a server *[figure 1, ref. Num "12"]* **with which the participants computing device** *[figure 1, ref. Num "14-16]* **is in communication.** *[figure 1, ref. Num "18" and See also page 5, under the title "Remote Attestation, up to page 6, first paragraph] ("TCPA remote attestation allows an application* ***(the "challenger")*** *to trust a remote platform. This trust is built by obtaining integrity metrics for the remote platform, securely storing these metrics and then ensuring that the reporting of the metrics is secure. For example, before making content available to a subscriber, it is likely that a service provider will need to know that the remote platform* ***is trustworthy.*** *The service provider's platform (the "challenger") queries " the remote platform, meets the limitation* ***"issuing a first challenge to a participant's computing device to determine whether the participant's computing device is trustworthy,"*** *During system boot, the challenged platform creates a cryptographic hash of the system BIOS, using an algorithm to create a statistically unique identifier for the platform. The integrity metrics are then stored. When it receives the query from the challenger, the remote platform responds by digitally signing and then sending the integrity metrics. The digital signature prevents tampering and allows the challenger to verify the signature. If the signature is verified, the challenger can then determine whether the identity metrics are trustworthy meets the limitation of* ***"determining whether or not the participant's computing device is trustworthy"*** *If so, the challenger, in this case the service provider, can then deliver the content. It is important to note that the TCPA process does not make judgments regarding the integrity metrics. It merely reports the metrics and lets the challenger* ***make the final decision regarding the trustworthiness*** *of the remote platform.)*

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
02/27/2007

Benjamin E Lanier
Examiner AU 2132